TOKEN2 Sàrl
Geneva, Switzerland
www.token2.com

Token2 Molto-1-i Multi-profile TOTP hardware token

Part no: Molto1-i · T2-61

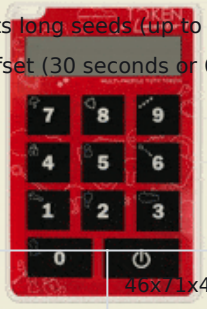





Description

dware token. Having a multi-profile programmable hardware token means you can have only one device for up to 10 of your accounts.

Molto-1-i supports long seeds (up to 128 base32 chars) and can be configured with different hash types (sha1 or sha256), time offset (30 seconds or 60 seconds), number of digits (6 or 8 digits) and an optional PIN code protection



Specifications

Dimensions	46x71x4mm
TOTP Profiles	up to 10
Programmable	via NFC using Windows, iPhone, Android app or cross-platform Python script
Time sync	Yes
NFC Access	Password protected - password can be changed

Time step	30 or 60 seconds
OTP Length	4, 6, 8 or 10 digits
Maximal seed length	160 HEX (128 base32)
Seed hash algorithm	SHA-1 or SHA-256
Extra security	PIN protection - OTPs will not show without the correct PIN code entered

Burning/programming/configuring the Molto-1-i token is done via NFC using a special burner app. We currently have iPhone, Windows and Android versions of the burner app as well as a cross-platform Python script that will allow to provision the device under Linux and macOS as well.

Windows App guide Android App guide
iPhone App guide Python script

FAQ

Q. What is the difference between Molto-1-i and Molto-1 ?

A. Molto-1-i works with Android, Windows and iPhone apps as well as the python script . Molto-1 supports only Windows and Android apps. Additionally, Molto-1-i has PIN protection feature.

Q. How secure is the procedure of programming/seeding the Molto-1-i via NFC?

A. There is absolutely no way to retrieve the seeds anyhow from the device. However, to fully ensure security, in particular, to prevent replay attack by modifying the system time (which is a highly demanded feature to solve the time drift issues) Molto-1 can be protected by setting an NFC access password. New devices will come with a default NFC access password which can be changed immediately. To prevent brute-force attack, the devices will be reset to factory defaults after around 100 unsuccessful NFC access attempts.

Q. What if I have set an NFC access password and forgot it. Does it mean that I can no longer use Molto-1?

A. No, you can still use it by resetting to factory default. This reset will set NFC access password to default, but the operation will also clear all TOTP profiles (seeds and settings).

Q. How long does the battery last?

A. Battery life depends on usage. Burning/programming operations via NFC consume a lot more power, so we must take that into account as well. As a rough estimation, if a token is used a few times per day (i.e. each profile is used once - so 10 button presses a day) and the NFC operations are not very frequent (i.e. not more than once a month) - the Molto-1 token will last for 4-5 years.

Q. Will I lose access to the TOTP profiles when the battery is dead?

A. Yes, but you will have enough time to prepare. Molto-1 will have a battery indicator on the display (). The indicator will show the status throughout the life of the token () . You should replace your token (and migrate the TOTP tokens by resetting the second factor on each respective service) when the indicator shows the battery level as "empty" () - you will still have a couple of months to do this.

Specifications

GENERAL	
Form factor	Multi-profile token
Interface	NFC
CONNECTIVITY	
USB-C	No
NFC	Yes
OTP	
OTP protocols	TOTP
TOTP	Yes
Programmable	Yes
Multi-profile	Yes
DIMENSIONS	
Dimensions	46 x 71 x 4 mm